Cross-Account Infrastructure Report

Customer: meridian-logistics-a1b2c3d4 | Accounts: 5 | Date: 2026-04-15

Overall Status

RED

Executive Summary

This week's report covers 5 accounts with a total estimated cost of $17,497/month — up $290 from last week, driven by increased Kinesis throughput in the ingestion account. Overall status remains RED. One production certificate is now 11 days from expiry (down from 18 days last week). Two items from last week's report have been resolved: Jenkins and Nexus instances in hub now have auto-stop schedules in place, recovering ~$340/month, and the IAM account password policy in hub has been corrected. Three new findings are raised this week: a worsening SQS DLQ backlog in ingestion, Kinesis shard utilisation approaching throttle, and IAM Identity Centre is absent across all accounts. Six findings from last week remain open.

Account Summaries

production (471000000004)

RED

Production remains RED this week. The ACM certificate on app.meridianlogistics.com.au is now 11 days from expiry — down from 18 days last week. Auto-renewal is not enabled. The PostgreSQL security group with public internet access remains open since 22 March. All other warnings carry over from the previous report.

Critical Findings

1. ACM certificate expiry — 11 days remaining

Certificate for app.meridianlogistics.com.au expires 2026-04-26. Was at 18 days last week — worsening. Auto-renewal via DNS validation is not enabled.

Impact: HTTPS will fail for all customer-facing traffic when the certificate lapses. Browser security warnings will appear 3 days prior.

Action: Enable DNS validation auto-renewal in ACM immediately, or upload a new certificate. Estimated fix time: 30 minutes.

2. Security group allows public internet access to PostgreSQL

Security group sg-0a4f2c1d has an inbound rule permitting TCP 5432 from 0.0.0.0/0. Open since 22 March 2026 — no action taken across two report cycles.

Impact: PostgreSQL is exposed to brute-force and credential stuffing attacks from the public internet. A single credential leak could result in a full database breach.

Action: Replace the 0.0.0.0/0 CIDR with the specific subnet CIDR of the application layer (e.g., 10.0.1.0/24). No downtime required.

Warnings

1. RDS storage at 87% — autoscaling not enabled

ml-prod-pg-primary (db.r6g.2xlarge) is using 87% of allocated storage. Storage autoscaling is disabled. Open since 8 April 2026.

Impact: RDS will become read-only and refuse writes when storage is full. At current growth rate, this could occur within 2–3 weeks.

Action: Enable RDS storage autoscaling with a maximum threshold of 500 GB. Alternatively, manually increase storage allocation now.

2. 3 IAM users with console access have no MFA

Users dev-ops-james, ml-admin-backup, and ci-deploy have AWS Console login enabled but no MFA device registered. Open since initial scan 1 April 2026.

Impact: A compromised password grants full console access to the production account with no second factor.

Action: Enforce MFA via IAM policy. Use aws iam list-users and get-login-profile to identify affected users, then require MFA via a Deny policy on aws:MultiFactorAuthPresent.

3. No CloudWatch alarms on RDS CPU or free storage

ml-prod-pg-primary has no alarms configured for CPUUtilization, FreeStorageSpace, or DatabaseConnections. Open since initial scan 1 April 2026.

Impact: Storage full events, CPU spikes, or connection exhaustion will not trigger any alert. On-call engineers will only learn of issues from customer complaints.
Action: Create alarms for: FreeStorageSpace < 20 GB, CPUUtilization > 80% for 5 minutes, DatabaseConnections > 80% of max_connections.

Estimated 30-day cost: $9240.00

---

ingestion (471000000005)

AMBER

The SQS DLQ backlog for EDI parse failures has grown from 843 messages last week to 1,247 this week — a 48% increase. Kinesis shard utilisation reached 89% following the onboarding of a new freight partner, raising a new throttle risk. CloudTrail and Lambda DLQ findings carry over from last week.

Critical Findings

1. SQS DLQ backlog growing — 1,247 unprocessed messages

Queue ml-ingest-failed contains 1,247 messages as of this report, up from 843 last week (+48%). These are EDI parse failures accumulating silently with no alerting configured.
Impact: Freight partner EDI transmissions are being silently dropped. Downstream order records in the production database are incomplete. This may be causing unreported reconciliation failures.
Action: Investigate parse failures by sampling messages from the DLQ. Add a CloudWatch alarm on ApproximateNumberOfMessages > 100. Review Lambda ml-edi-parser error logs for recurring failure patterns.

Warnings

1. Lambda ml-edi-parser has no DLQ configured

The Lambda function handling EDI intake has no dead-letter queue. Failed async invocations are silently dropped after the retry policy exhausts. Open since initial scan 1 April 2026.
Impact: If the Lambda fails asynchronously (e.g., from a Kinesis trigger), the payload is lost with no record. This masks data loss and makes root-cause analysis difficult.
Action: Add a DLQ (SQS) to ml-edi-parser. Set FunctionResponseTypes to ReportBatchItemFailures on the Kinesis trigger to allow partial failure reporting.

2. Kinesis stream at 89% shard utilisation — approaching throttle

Stream ml-partner-events is at 89% of provisioned shard capacity. A new freight partner was onboarded this week, increasing ingest throughput. New finding this week.
Impact: At current growth rate, the stream will hit the shard limit within days, causing ProvisionedThroughputExceededException errors. EDI messages will be dropped or delayed.
Action: Increase shard count from current provisioned value (check DescribeStream) or enable Kinesis On-Demand mode to handle variable throughput automatically.

3. CloudTrail not enabled in ap-southeast-2

No CloudTrail trail is active in ap-southeast-2 for this account. API activity in the ingestion account has no audit log. Open since initial scan 1 April 2026.
Impact: Any unauthorised API calls, data exfiltration, or misconfiguration events in this account will leave no forensic trail.
Action: Create a multi-region CloudTrail trail logging to a dedicated S3 bucket with MFA delete enabled. Estimated setup time: 15 minutes via console or CLI.

Estimated 30-day cost: $3870.00

---

hub (471000000003)

AMBER

Two findings resolved since last week: Jenkins and Nexus instances now have auto-stop schedules, recovering ~$340/month in EC2 spend, and the IAM account password policy has been corrected (minimum 14 characters, 90-day rotation). Two warnings remain open: NAT Gateway single-AZ placement and unrestricted security group egress.

Warnings

1. NAT Gateway in single AZ — single point of failure

The NAT Gateway is deployed in ap-southeast-2a only. All outbound internet traffic from the hub VPC routes through a single AZ. Open since initial scan 1 April 2026.
Impact: An AZ failure in ap-southeast-2a will cut outbound internet access for all resources in hub, including CI/CD pipelines, Active Directory external lookups, and monitoring agents.
Action: Deploy a second NAT Gateway in ap-southeast-2b and update route tables for subnets in that AZ. Monthly cost increase: ~$35.

2. 4 security groups with unrestricted egress

Security groups sg-hub-jenkins, sg-hub-nexus, sg-hub-monitoring, and sg-hub-vpn have outbound rules permitting all traffic to 0.0.0.0/0 on all ports. Open since 8 April 2026.

Impact: Unrestricted egress makes it easier for a compromised instance to exfiltrate data or communicate with command-and-control infrastructure.

Action: Restrict egress to known destinations: HTTPS (443) to specific CIDRs for CI/CD dependencies, Nexus mirror, and monitoring endpoints. Remove catch-all egress rules.

Estimated 30-day cost: $1840.00

---

uat (471000000002)

GREEN

UAT remains GREEN with no critical findings. Three low-priority warnings carry over from the previous report. No new findings this week.

Warnings

1. 3 EC2 instances stopped for over 45 days

Instances i-0abc1234 (ml-uat-worker-1), i-0def5678 (ml-uat-worker-2), and i-0ghi9012 (ml-uat-bastion-old) have been stopped since 28 February 2026. EBS volumes remain attached and billed. Open since initial scan 1 April 2026.

Impact: Approximately $85/month is being spent on EBS volumes for instances with no indication of planned restart.

Action: Verify with the UAT team whether these instances are still needed. If not, create snapshots then terminate the instances to stop EBS billing.

2. RDS instance oversized — averaging 6% CPU

ml-uat-pg (db.t3.medium) has averaged 6% CPUUtilization over the past 30 days. Open since 8 April 2026.

Impact: Approximately $180/month is being spent on an RDS instance significantly larger than the UAT workload requires.

Action: Downsize to db.t3.small during the next scheduled maintenance window. Estimated saving: $90/month.

3. 7 S3 buckets with no lifecycle policies

Buckets ml-uat-artifacts, ml-uat-logs, ml-uat-exports, ml-uat-cache, ml-uat-backups, ml-uat-test-data, and ml-uat-reports have no lifecycle rules configured. Open since initial scan 1 April 2026.

Impact: Test data, logs, and build artefacts accumulate indefinitely. S3 storage costs in UAT will grow unbounded.

Action: Add a lifecycle rule to each bucket: transition objects to S3 Intelligent-Tiering after 30 days, expire after 90 days.

Estimated 30-day cost: $1340.00

---

sandbox (471000000001)

AMBER

Sandbox carries four open warnings from previous reports. A new EC2 dev instance was added Friday, increasing the account cost from $867 to $1,207 this week. No new security findings. All four warnings from last week remain unaddressed.

Warnings

1. IAM password policy not configured

No account-level IAM password policy exists. Developers can set any password including single-character strings with no rotation requirement. Open since initial scan 1 April 2026.

Impact: Weak developer credentials in the sandbox account could be used as an entry point via credential stuffing or social engineering.

Action: Apply an IAM password policy: minimum 14 characters, require numbers and symbols, 90-day maximum age, prevent reuse of last 5 passwords.

2. CloudTrail not enabled — no developer activity audit trail

No CloudTrail trail is active in the sandbox account. All developer API actions — including IAM changes, S3 access, and EC2 operations — go unlogged. Open since initial scan 1 April 2026.

Impact: If a developer misconfigures a resource or introduces a security issue, there is no trail to identify when it happened, what changed, or who made the change.

Action: Enable a multi-region CloudTrail trail with S3 log delivery. Cost: approximately $2/month for a low-activity sandbox.

3. 8 EC2 dev instances running 24/7 with no schedule

8 developer EC2 instances (t3.medium to t3.large) have been running continuously with no Instance Scheduler tags. No schedule tags detected. Open since initial scan 1 April 2026.

Impact: Estimated $520/month in avoidable EC2 spend assuming 8-hour weekday usage pattern. Instances are idle on nights and weekends.

Action: Apply Instance Scheduler or SSM Maintenance Window tags to power down outside business hours. Alternatively, use AWS Instance Scheduler CDK construct for automatic weeknight/weekend shutdown.

4. No AWS Budgets alerts configured

No budget or cost alert exists for the sandbox account. Cost spikes from runaway dev instances or accidental resource creation will not trigger any notification. Open since initial scan 1 April 2026.

Impact: A developer could inadvertently launch high-cost resources (GPU instances, Redshift clusters) and the cost would only be discovered at month end.

Action: Create a monthly budget of $1,500 with email alerts at 80% and 100%. Use aws budgets create-budget.

Estimated 30-day cost: $1207.00

Cross-Account Findings

1. No consistent resource tagging across accounts

14 different tag key schemas were identified across 5 accounts. Common tags such as Environment, Owner, and CostCentre are applied inconsistently or missing entirely. Open since initial scan 1 April 2026.

Impact: Cost allocation by team or project is unreliable. AWS Cost Explorer tag-based grouping returns incomplete data, making it difficult to attribute the $17,497/month total to individual teams or workloads.

Action: Define a standard tag schema (Environment, Owner, CostCentre, Project) and enforce via AWS Config managed rule required-tags across all accounts.

2. IAM Identity Centre not configured — 23 direct IAM users across accounts

23 individual IAM users have been identified across the 5 accounts with no SSO or Identity Centre in use. New finding this week identified during cross-account IAM audit.

Impact: Each IAM user is an independent credential that must be managed and rotated separately. A single compromised credential gives access to one account without cross-account visibility. Off-boarding an employee requires manual IAM user deletion in each account.

Action: Deploy AWS IAM Identity Centre (successor to SSO) in the management account. Migrate all human access to SSO permission sets. Remove direct IAM users from all member accounts.

3. AWS Config not enabled in any account

DescribeConfigurationRecorders returns no active recorders in all 5 accounts. No AWS managed rules, no configuration drift detection, and no compliance baseline are in place. Open since initial scan 1 April 2026.

Impact: Infrastructure drift, security group changes, and IAM policy modifications are not tracked. There is no automated compliance check against CIS benchmarks or internal security standards.

Action: Enable AWS Config in all accounts with a conformance pack (e.g., Operational Best Practices for CIS AWS Foundations). Use AWS Organizations to deploy Config centrally. Estimated monthly cost: ~$8 per account.

4. Backup coverage gap — ingestion, hub, and sandbox have no automated backup strategy

AWS Backup plans exist only for the production RDS instance. The ingestion account (Kinesis configuration, Lambda code), hub account (Active Directory, Jenkins configuration), and sandbox account have no backup plans. Open since initial scan 1 April 2026.

Impact: A data loss event or accidental deletion in ingestion, hub, or sandbox would require manual reconstruction. The hub account contains Active Directory and CI/CD configuration that would take days to rebuild.

Action: Create AWS Backup plans for all RDS instances and EBS volumes across ingestion and hub accounts. Add daily snapshots with 30-day retention. Estimated monthly cost: ~$15.

Recommendations

[HIGH] 1. Renew ACM certificate on production immediately
Certificate for app.meridianlogistics.com.au expires in 11 days. Enable DNS validation auto-renewal in ACM. This takes 30 minutes and prevents a customer-facing outage.

[HIGH] 2. Remove public internet access from PostgreSQL security group
Replace the 0.0.0.0/0 rule on sg-0a4f2c1d with the application subnet CIDR. Open since 22 March. No downtime required.

[MEDIUM] 3. Drain and investigate the SQS DLQ backlog in ingestion
1,247 EDI parse failures are accumulating. Sample failed messages, identify the root cause in ml-edi-parser, then add alerting so future failures are caught immediately.

[MEDIUM] 4. Deploy IAM Identity Centre and remove direct IAM users
23 direct IAM users across 5 accounts. Centralise access via IAM Identity Centre with permission sets. Reduces off-boarding risk and simplifies access audits.

This report was generated using read-only AWS API access. No changes were made to your infrastructure. For support, contact support@triont.com.